



Quick Snapshot of All Your Sites

The mySites.guru snapshot runs 140+ best-practice checks - PHP version, CMS config, security headers, SSL and more - twice a day on every connected site.

Phil E. Taylor | 26 March 2026

The mySites.guru **snapshot** runs automatically twice a day - or on demand - across every site in your account. Over 140 data points, collected in seconds. PHP version, CMS config, user accounts, security headers, the lot.

It's not a photo of your site. It's a fast check of what's configured properly and what isn't.

What exactly is the mySites.guru snapshot?

Within mySites.guru, where you can add unlimited Joomla and WordPress sites to your account, you'll see two main areas of checks on the Manage Site page: the **Snapshot** and the **Audit**.

The snapshot checks complete within milliseconds. The audit goes deeper - inspecting every line of code in every file on your webspace - so it takes longer.

Both give you a long list of best-practice checks and flag the things that need attention.

The snapshot covers your platform (Joomla/WordPress) configuration, writing settings, discussion settings, user accounts and access, plugins and extensions, file information, database integrity, and hosting environment.

Each check displays the current status on your site, the trend (whether it's changed, increased, or decreased), a Learn More button, and either a quick toggle or a link to the investigation page where you can dig into the reported issue and fix it.



The screenshots below are from an older version of the interface. We've since redesigned the dashboard, but the process works the same way.

Can You Resolve Problems with a Single Click?

Some of the Discussion Settings checks for WordPress:



On the right you can see that these checks can be resolved with a toggle switch - a single click and your site is following best practice again.

How Often Does the Snapshot Run?

Once a site is connected to mySites.guru, the snapshot data refreshes automatically twice a day. Hit "Take a new snapshot" any time you want fresh data.

A huge number of checks

We check everything we consider best practice for secure and well-configured websites. You might not agree with every recommendation, and that's fine.

One section of the Joomla snapshot:

OK	⚠️ Dont Leave WP_DEBUG Development Mode On	Learn	✓	<input type="checkbox"/>
OK	⚠️ Dont Leave WP_DEBUG_LOG Development Mode On	Learn	✓	<input type="checkbox"/>
OK	⚠️ Dont Leave WP_DEBUG_DISPLAY Development Mode On	Learn	✓	<input type="checkbox"/>
1 Issue	⚠️ Disable File Editing Through Admin Console With DISALLOW_FILE_EDIT	Learn	✗	<input type="checkbox"/>
OK	⚠️ Enable FORCE_SSL_ADMIN To Secure Admin Connections	Learn	✓	<input type="checkbox"/>
1 Issue	⚠️ Enable FORCE_SSL_LOGIN To Secure Login Connections (@Deprecated)	Learn	✗	<input type="checkbox"/>
OK	⚠️ Prohibit Database Repair With WP_ALLOW_REPAIR Constant	Learn	✓	<input type="checkbox"/>
1 Issue	⚠️ Disallow Unfiltered Content With DISALLOW_UNFILTERED_HTML	Learn	✗	<input type="checkbox"/>
1 Issue	⚠️ Disable Unfiltered File Uploads With ALLOW_UNFILTERED_UPLOADS	Learn	✗	<input type="checkbox"/>
1 Issue	⚠️ Enable Auto Upgrades With AUTOMATIC_UPDATER_DISABLED Constant	Learn	✗	<input type="checkbox"/>
OK	⚠️ Enable Minor Upgrades Only With WP_AUTO_UPDATE_CORE Constant	Learn	✓	<input type="checkbox"/>
1 Issue	⚠️ Disable Plugin Installs With DISALLOW_FILE_MODS Constant	Learn	✗	<input type="checkbox"/>
OK	⚠️ Disable Script Debugging With SCRIPT_DEBUG Constant	Learn	✓	<input type="checkbox"/>
OK	⚠️ Disable Save Queries Debug With SAVEQUERIES Constant	Learn	✓	<input type="checkbox"/>
1 Issue	⚠️ Enable WP_POST_REVISIONS To Limit Number Of Revisions Saved To 10	Learn	✗	<input type="checkbox"/>
1 Issue	⚠️ Set AUTOSAVE_INTERVAL To 30 Seconds To Prevent Data Loss	Learn	✗	<input type="checkbox"/>

And the full page view (if you have good eyesight):

myValentines! 🔍 Search for a tool, site, feature - everything. Report Page Inconsistency Ask for Support

Find a Tool **Karl Brown** Site Admin Login

WordPress Configuration

WordPress Version Must Be Up-to-date Learn Investigate

Use A Valid SSL Certificate To Secure Traffic Learn Investigate

WordPress Address Should Normally Equal Site Address Learn Investigate

Disable XML-RPC In WordPress Learn Investigate

Don't Encourage Search Engines From Indexing This Site Learn Investigate

Don't Use The Default Distributor (jet-pack) Learn Investigate

Remove Default Tag Line "Just Another WordPress Site" Learn Investigate

Remove The Default "Sample Page" Learn Investigate

Remove The Default "Hello World" Post Learn Investigate

Don't Leave WP_DEBUG Development Mode On Learn Investigate

Don't Leave WP_DEBUG_DISPLAY Development Mode On Learn Investigate

Disable File Editing Through Admin Console With SCRIPT_DEBUG Learn Investigate

Enable SCRIPT_DEBUG To Secure Admin Connections Learn Investigate

Enable SCRIPT_DEBUG To Secure Login Connections (obscure) Learn Investigate

Prevent Database Escape With WP_ALLOW_SCRIPTS Constant Learn Investigate

Disable Unrelated Content With DISALLOW_EXTERNAL_SCRIPTS Learn Investigate

Disable Unrelated File Uploads With ALLOW_MULTIMEDIA_UPLOADS Learn Investigate

Enable Auto-Updates With AUTOMATIC_UPDATES_DISABLED Constant Learn Investigate

Enable Minor Updates Only With WP_AUTO_UPDATE_CORE Constant Learn Investigate

Disable Plugin Installs With DISALLOW_PLUGIN_INSTALL Constant Learn Investigate

Disable Script Debugging With SCRIPT_DEBUG Constant Learn Investigate

Disable File Uploads With ALLOW_UPLOADS Constant Learn Investigate

Enable WP_DEBUG_DISPLAY To Limit Number Of Comments Saved To DB Learn Investigate

Use WP_DEBUG_DISPLAY To 30 seconds To Prevent Data Loss Learn Investigate

Disable Scripts Learn Investigate

Remove jQuery Migrate Script Learn Investigate

Remove WordPress Admin Footer Banner Learn Investigate

Remove WordPress & Other Plugins Generator Tags/Version Numbers Learn Investigate

Remove Feed Shortlink Head Tags Learn Investigate

Remove WordPress Logo Menu Top Left Of Admin Console Learn Investigate

Disable WordPress Application Passwords For APIs Learn Investigate

Disable Links In User Comments To Hide Spam Learn Investigate

Disable The "Blog" -> Grouping Learn Investigate

Remove As Many Admin Page Screens From Plugins As We Can! Learn Investigate

Disable The Menu Bar On The Frontend, When Logged In Learn Investigate

Appearance

Do Not Use Default Themes Learn Investigate

Writing Settings

Default Post Category Should Not Be Uncategorized Learn Investigate

Post Via Email Settings Should Be Removed Unless Required Learn Investigate

Remove Old Post Revisions From The Database Learn Investigate

Remove Auto-Save Revisions From The Database Learn Investigate

Remove Trashed Posts And Pages From The Database Learn Investigate

Remove Draft Posts And Pages From The Database Learn Investigate

Discussion Settings

Disable Allowing People To Post Comments On New Articles Learn Investigate

Enable Comment Author Must Fill Out Name And Email Learn Investigate

Disable "Users Must Be Registered And Logged In To Comment" Learn Investigate

Reduce Number Of Comments Requiring Moderation In DB Learn Investigate

Keep Number Of Comments In The DB At Zero Learn Investigate

User Accounts And Access

"Anyone Can Register" Should Be Disabled Unless Required Learn Investigate

New User Default Role Should Not Be Administrator Learn Investigate

Limit The Number Of Administrators To One Learn Investigate

Don't Use "admin" As A Username Learn Investigate

Privacy: Keep Pending/Export Requests At Zero Learn Investigate

Privacy: Remove Completed/Export Requests Learn Investigate

Privacy: Keep Pending/Remove Requests At Zero Learn Investigate

Privacy: Remove Completed/Remove Requests Learn Investigate

Plugins

Delete The Files For Disabled Plugins Learn Investigate

File Information

Investigate And Remove Jpeg-compatibility.jpg Learn Investigate

Database Integrity

Default Database Profile Should Not Be Set As wp_ Learn Investigate

Database User Should Not Be "root" Learn Investigate

DB User Should Only Have Access To One Database Learn Investigate

Response Security Headers Information

X-Frame-Options: DENY - New Header To Control Which Features And APIs Can Be Used In The Browser Learn Investigate

Remove Deprecation: X-Frame-Options: DENY Header Learn Investigate

Set X-Frame-Options: DENY - Set How Much Info Is Leaked When Logging Away From Site Learn Investigate

Set X-Frame-Options: DENY - Set To Policy Enforces The Use Of HTML5 Learn Investigate

X-Content-Type-Options: nosniff - Stops A Browser From Trying To sniff the Content Type Learn Investigate

X-Frame-Options: SAMEORIGIN - Tells The Browser Whether You Want To Allow Your Site To Be Framed Or Not Learn Investigate

Hosting Environment

PHP Version Number Should Be Latest Learn Investigate

PHP Safe Mode Should Be Off Learn Investigate

PHP Display Errors Configuration Should Be Off Learn Investigate

PHP Register Globals Should Be Off Learn Investigate

PHP File Uploads Should Be Enabled Learn Investigate



That's just some of the snapshot checks.

What Other Features Does the Snapshot Power?

At the end of each snapshot, mySites.guru gathers a list of your extensions, plugins, templates, and themes, then checks each one for available updates. This data feeds into tools like the [Active Theme and Template List](#), which lets you see and compare every site's template across your entire portfolio.

Depending on your settings, you can enable [automatic updates](#) for these - but that's a topic for another post.

The snapshot also captures your site version, PHP version, and other environment details that feed into the dashboard overview. For Joomla 5 and 6 sites, it checks for [locked scheduled tasks](#) that can silently break background jobs like update notifications and backups.

Can the Snapshot Identify Hacks?

The snapshot isn't designed to find hacks - that's the [security audit's](#) job. But it does catch things. We push new checks frequently, and when we spot attack trends, we add checks for those too.

For example, there was a specific attack that created usernames matching the pattern `Joomla.user.helper.XXXX`. You probably wouldn't notice one suspicious username among thousands of users - but the mySites.guru snapshot would, flagging it for you to investigate.

For a broader look at the security checks behind the snapshot, see the [WordPress and Joomla security guide](#).

Frequently Asked Questions

What is the mySites.guru snapshot and how often does it run?

The snapshot is an automated collection of over 140 best practice and security data points - covering PHP version, CMS configuration, user accounts, and more - run automatically twice a day and available on demand.

What is the difference between the snapshot and the audit in mySites.guru?

The snapshot completes in milliseconds by checking configuration and settings, while the audit performs a deeper inspection of every file and line of code in your webspace to find malware and hidden threats.

Can I fix issues found in the snapshot without leaving mySites.guru?

Yes - many snapshot checks include a quick toggle switch that applies the recommended fix to your site with a single click directly from the dashboard.

What does the snapshot check on my WordPress or Joomla site?

The snapshot checks platform configuration, writing settings, discussion settings, user accounts, plugins and extensions, file information, database integrity, hosting environment, PHP version, and SSL certificates.

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



mySites.guru

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru